UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,703	12/21/1999	XI WANG	D/99192	3974

7590 07/12/2004

NIXON PEABODY LLP
8180 GREENBORO DRIVE
SUITE 800
MCLEAN, VA 22102

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/12/2004

11

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/468,703	WANG, XI	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 6-10.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 have been examined.

2. Claims 1, 4-7, 12-17, and 19-20 are rejected under 35 U.S.C. 102(e) and Claims 2-3, 8-11, and 18 are rejected under 35 U.S.C. 103(a).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 4-7, 12-17, and 19-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Wiser, Et Al. (US 6,385,596).

As per claim 1:

Wiser, Et Al. disclose a public, non-commutative method for encoding an original message to be passed a recipient by way of a grantor, the method comprising the steps of:

obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor; **[col.7, lines 38-40]**

generating a public proxy key based on a private key corresponding to the recipient, wherein it is computationally difficult to recover the private key corresponding to the recipient from the public proxy key; and **[col.7, lines 43-45 and col.10, lines 23-25]**

applying the public proxy key to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and any available public information. **[col.9, lines 30-35 and col.12, lines 30-52]**

As per claim 4 : See col.9, lines 4-10 and col.10, lines 18-34; discusses the receiving, generating, and applying steps are performed by the grantor.

As per claim 5: See col.9, lines 42-47; discussing the providing the transformed message to the recipient.

As per claim 6: See col.9, lines 25-37; discusses decrypting the transformed message using information selected from the private key corresponding to the recipient and any available public information.

As per claim 7: See col.10, lines 23-29; discusses decrypting the transformed message using information using the private key corresponding to the recipient.

As per claim 12: See col.12, lines 5-18 and col.13, lines 47-52; discussing the encrypted message comprises a first portion and a second portion, the first portion encoding the original message, a generator, and a random key, and the second portion encoding the public key corresponding to the grantor and the random key.

As per claim13: See col.10, lines 27-29; discussing the applying step operates on the second portion of the encrypted message.

As per claim14: See col., lines ; discussing the original message is passed to a recipient through at least one additional intermediate grantor by repeating the generating and applying steps for each additional intermediate grantor.

As per claim 15:

Wiser disclose a public, non-commutative method for encrypting an original message to be passed a recipient by way of a grantor, the method comprising the steps of:

obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor; **[col.7, lines 38-40]**

transforming the encrypted message, using a transformation key corresponding to the recipient, into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and any available public information. **[col.7, lines 43-45 and col.10, lines 23-25]**

As per claim 16: See col.13, lines 51-52; discussing the transformation key comprises a private key corresponding to the recipient.

As per claim 17: See col.13, lines 547-49; discussing the transformation key comprises a public key corresponding to the recipient.

As per claim 19: See col.10, lines 23-29; discussing the message is decryptable by the recipient using information selected from the private key corresponding to the recipient.

As per claim 20: See col.10, lines 18-35 and col.13, line 63 thru col.14, line 4; discussing the original message is passed to a recipient through at least one additional intermediate grantor by repeating the transforming step for each additional intermediate grantor.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2-3, 8-11, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser, Et Al., and further in view of Mittra (US 5,748,736).

As per claim 2:

Wiser discloses digitally signing a message (col.21, lines 48-52) with the teachings of having a encrypted original message and a public key based on a private key that corresponds to the recipient wherein re-encrypting using the public (proxy) key to transform the encrypted message into a transformed message (col.13, line 56 thru col.14, line 13). However, Wiser fails to include an ElGamal encryption scheme.

Mittra teaches decrypting the encrypted message and then re-encrypting the message along with digitally signing the messages. Mittra discloses that the procedures of digitally signing the messages such as the DSS and the ElGamal signature schemes are well known in the art for supporting

source authentication and sender non-repudiation (col.10, line 62 thru col.11, line 3).

Therefore, it would have been obvious for a person of ordinary skill in the art to modify Wiser to include the ElGamal encryption scheme because digitally signing the messages supports authentication and sender non-repudiation.

As per claim 3:

Wiser discloses digitally signing a message (col.21, lines 48-52) with the teachings of having a encrypted original message and a public key based on a private key that corresponds to the recipient wherein re-encrypting using the public (proxy) key to transform the encrypted message into a transformed message (col.13, line 56 thru col.14, line 13). However, Wiser fails to include a modified ElGamal encryption scheme.

Mittra teaches decrypting the encrypted message and then re-encrypting the message along with digitally signing the messages. Mittra discloses that the procedures of digitally signing the messages such as the DSS and the ElGamal signature schemes are well known in the art for supporting source authentication and sender non-repudiation (col.10, line 62 thru col.11, line 3).

Therefore, it would have been obvious for a person of ordinary skill in the art to modify Wiser to include the ElGamal encryption scheme because digitally signing the messages supports authentication and sender non-repudiation.

As per claim 8: Wiser discusses the encrypted message comprises a first portion and a second portion, the first portion encoding a generator and a random key, and the second portion encoding the original message, the public key corresponding to the grantor, and the random key (col.12, lines 5-18 and col.13, lines 47-52).

As per claim 9: See Wiser on col.10, lines 27-29; discussing the applying step operates on the second portion of the encrypted message.

As per claim 10: Wiser discusses the encrypted message comprises a first portion and a second portion, the first portion encoding the original message, a generator, and a random key, and the second portion encoding the public key corresponding to the grantor and the random key (col.12, lines 5-18 and col.13, lines 47-52).

As per claim 11: See Wiser on col.10, lines 27-29; discussing the applying step operates on the second portion of the encrypted message.

As per claim 18: Although, Wiser fails to include the ElGamal or the Cramer-Shoup encryption scheme, it is obvious to use anyone of these encryption schemes for purposes of additional security.

***For more details and information concerning the rejection above, please refer to Wiser, Et Al. on col.3, line 5...Et. SEQ. and Mittra on col.4, line 5...Et. SEQ.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

LHa